Results for "(((hamming weight<in>metadata)<and>(ring<in>metadata))<and>(integer<in>metadata))" e-mail
Your search matched **2** of **9** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

» View Session History

» New Search

Modify Search

((((hamming weight<in>metadata)<and>(ring<in>metadata))<and>(integer<in>metac

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL IEEE Journal or Magazine

IEE JNL IEE Journal or Magazine

IEEE CNF IEEE Conference Proceeding

IEE CNF IEE Conference Proceeding

IEEE STD IEEE Standard

Select Article Information

1. **On the weight hierarchy of Goethals codes over Z_4**
Kyeongcheol Yang; Helleseth, T.;
Information Theory, IEEE Transactions on
Volume 44, Issue 1, Jan. 1998 Page(s):304 - 307
AbstractPlus | References | Full Text: PDF(212 KB) IEEE JNL

2. **A 2-adic approach to the analysis of cyclic codes**
Calderbank, A.R.; Wen-Ching Winnie Li; Poonen, B.;
Information Theory, IEEE Transactions on
Volume 43, Issue 3, May 1997 Page(s):977 - 986
AbstractPlus | References | Full Text: PDF(568 KB) IEEE JNL

Terms used **hamming weight** and **ring** and **integer** and **sets** and **module** and **digital operator** and **certificate** and **signature**

Found **9,671** of **154,226**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 AReCA: a highly attack resilient certification authority

Jiwu Jing, Peng Liu, Dengguo Feng, Ji Xiang, Neng Gao, Jingqiang Lin

October 2003 **Proceedings of the 2003 ACM workshop on Survivable and self-regenerative systems: in association with 10th ACM Conference on Computer and Communications Security**

Full text available: pdf(1.40 MB) Additional Information: full citation, abstract, references, index terms

Certification Authorities (CA) are a critical component of a PKI. All the certificates issued by a CA will become invalid when the (signing) private key of the CA is compromised. Hence it is a very important issue to protect the private key of an online CA. ARECA systems, built on top of threshold cryptography, ensure the security of a CA through a series of defense-in-depth protections. ARECA systems won't be compromised when a few system components are compromised or some system administrat ...

Keywords: CA, RSA, attack resilience, digital signature, intrusion tolerance

2 A secure and private system for subscription-based remote services

Pino Persiano, Ivan Visconti

November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4

Full text available: pdf(241.65 KB) Additional Information: full citation, abstract, references, index terms

In this paper we study privacy issues regarding the use of the SSL/TLS protocol and X.509 certificates. Our main attention is placed on subscription-based remote services (e.g., subscription to newspapers and databases) where the service manager charges a flat fee for a period of time independent of the actual number of times the service is requested.We start by pointing out that restricting the access to such services by using X.509 certificates and the SSL/TLS protocol, while preserving the in ...

Keywords: Access control, anonymity, cryptographic algorithms and protocols, privacy, world-wide web

3 Trustworthy 100-year digital objects: Evidence after every witness is dead

Henry M. Gladney

July 2004 **ACM Transactions on Information Systems (TOIS)**, Volume 22 Issue 3

Full text available: pdf(1.24 MB) Additional Information: full citation, abstract, references, index terms

In ancient times, wax seals impressed with signet rings were affixed to documents as evidence of their authenticity. A digital counterpart is a message authentication code fixed firmly to each important document. If a digital object is sealed together with its own audit trail, each user can examine this evidence to decide whether to trust the content---no matter how distant this user is in time, space, and social affiliation from the document's source.We propose an architecture and design that a ...

4 Data Security

Dorothy E. Denning, Peter J. Denning

September 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 3

Full text available: pdf(1.97 MB) Additional Information: full citation, references, citings, index terms

5 1996 East Coast Computer Algebra Day Abstracts, Yorktown Heights, New York, April 13, 1996

March 1996 **ACM SIGSAM Bulletin**, Volume 30 Issue 1

Full text available: pdf(1.06 MB) Additional Information: full citation

6 Simple algebras are difficult

L. Ronyai

January 1987 **Proceedings of the nineteenth annual ACM conference on Theory of computing**

Full text available: pdf(1.29 MB) Additional Information: full citation, abstract, references, citings, index terms

Let F be a finite field or an algebraic number field. In previous work we have shown how to find the basic building blocks (the radical and the simple components) of a finite dimensional algebra over F in polynomial time (deterministically in characteristic zero and Las Vegas in the finite case). Here we address the more general problem of finding zero divisors in A. This problem is equivalent to finding a nontrivial common invariant subspa ...

7 Program Transformation Systems

H. Partsch, R. Steinbrüggen

September 1983 **ACM Computing Surveys (CSUR)**, Volume 15 Issue 3

Full text available: pdf(3.00 MB) Additional Information: full citation, references, citings, index terms

8 Session 8: Gossiping to reach consensus

Bogdan S. Chlebus, Dariusz R. Kowalski

August 2002 **Proceedings of the fourteenth annual ACM symposium on Parallel algorithms and architectures**

Full text available: pdf(237.65 KB) Additional Information: full citation, abstract, references, citings, index terms

We consider the problem of gossiping when dynamic node crashes are controlled by adaptive adversaries. We develop gossiping algorithms which are efficient with respect to both the time and communication measured as the number of point-to-point messages. If the adversary is allowed to fail up to t nodes, among the total of n, where additionally $n-t=\Omega(n/\textpolylog n)$, then one among our algorithms completes gossiping in

time $\cO(\log^2 t)$ and with $\cO(n\text polylog t)$ messages. W ...

Keywords: adaptive adversary, consensus, distributed algorithm, gossiping, lower bound, processor failures

9 Illustrative risks to the public in the use of computer systems and related technology

Peter G. Neumann

January 1996 **ACM SIGSOFT Software Engineering Notes**, Volume 21 Issue 1

Full text available: pdf(2.54 MB) Additional Information: full citation

10 The concept of dynamic analysis

Thoms Bell

October 1999 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 7th European software engineering conference held jointly with the 7th ACM SIGSOFT international symposium on Foundations of software engineering**, Volume 24 Issue 6

Full text available: pdf(1.37 MB) Additional Information: full citation, abstract, references, citings, index terms

Dynamic analysis is the analysis of the properties of a running program. In this paper, we explore two new dynamic analyses based on program profiling:Frequency Spectrum Analysis. We show how analyzing the frequencies of program entities in a single execution can help programmers to decompose a program, identify related computations, and find computations related to specific input and output characteristics of a program.Cover ...

11 Security and Middleware Services: Towards flexible credential verification in mobile ad-hoc networks

Sye Loong Keoh, Emil Lupu

October 2002 **Proceedings of the second ACM international workshop on Principles of mobile computing**

Full text available: pdf(281.24 KB) Additional Information: full citation, abstract, references, index terms

Ad-hoc networks facilitate interconnectivity between mobile devices without the support of a network infrastructure. In this paper we propose a flexible credential verification mechanism, which improves the likelihood that participants in an ad-hoc network can verify each other's credentials despite the lack of access to certification and attribute authorities. Users maintain Credential Assertion Statements (CASs), which are formed through extraction of X.509 and attribute certificates into an i ...

Keywords: authentication, credential verification, security, trust

12 A language for computational algebra

Richard D. Jenks, Barry M. Trager

August 1981 **Proceedings of the fourth ACM symposium on Symbolic and algebraic computation**

Full text available: pdf(507.92 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper reports ongoing research at the IBM Research Center on the development of a language with extensible parameterized types and generic operators for computational algebra. The language provides an abstract data type mechanism for defining algorithms which work in as general a setting as possible. The language is based on the notions of domains and categories. Domains represent algebraic structures. Categories designate

collections of domains ...

13 Technical contributions: A language for computational algebra
Richard D. Jenks, Barry M. Trager
November 1981 **ACM SIGPLAN Notices**, Volume 16 Issue 11

Full text available: pdf(543.73 KB) Additional Information: full citation, abstract, references

This paper reports ongoing research at the IBM Research Center on the development of a language with extensible parameterized types and generic operators for computational algebra. The language provides an abstract data type mechanism for defining algorithms which work in as general a setting as possible. The language is based on the notions of *domains* and *categories*. Domains represent algebraic structures. Categories designate collections of domains having common operations with s ...

14 Credentials: Direct anonymous attestation
Ernie Brickell, Jan Camenisch, Liqun Chen
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**

Full text available: pdf(314.67 KB) Additional Information: full citation, abstract, references, index terms

This paper describes the direct anonymous attestation scheme (DAA). This scheme was adopted by the Trusted Computing Group (TCG) as the method for remote authentication of a hardware module, called Trusted Platform Module (TPM), while preserving the privacy of the user of the platform that contains the module. DAA can be seen as a group signature without the feature that a signature can be opened, i.e., the anonymity is not revocable. Moreover, DAA allows for pseudonyms, i.e., for each signat ...

Keywords: anonymous credential systems, cryptographic protocols, integrity based computing, privacy, trusted computing

15 Illustrative risks to the public in the use of computer systems and related technology
Peter G. Neumann
January 1992 **ACM SIGSOFT Software Engineering Notes**, Volume 17 Issue 1

Full text available: pdf(1.65 MB) Additional Information: full citation, citings, index terms

16 Unified algebras and modules
P. D. Mosses
January 1989 **Proceedings of the 16th ACM SIGPLAN-SIGACT symposium on Principles of programming languages**

Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, references, index terms

This paper concerns the algebraic specification of abstract data types. It introduces and motivates the recently-developed framework of unified algebras, and provides a practical notation for their modular specification. It also compares unified algebras with the well-known framework of order-sorted algebras, which underlies the OBJ specification language.

17 Fast detection of communication patterns in distributed executions
Thomas Kunz, Michiel F. H. Seuren
November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research**

Full text available: pdf(4.21 MB) Additional Information: full citation, abstract, references, index terms

Understanding distributed applications is a tedious and difficult task. Visualizations based on

process-time diagrams are often used to obtain a better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the University of Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the application. In our experience, such tools display repeated occurrences of non-trivial commun ...

18 The new (1982) Computing Reviews classification system—final version

Jean E. Sammet, Anthony Ralston

January 1982 **Communications of the ACM**, Volume 25 Issue 1

Full text available: pdf(731.04 KB) Additional Information: full citation, citings, index terms

19 On randomization in sequential and distributed algorithms

Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar

March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1

Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms—both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

20 Typechecking and modules for multimethods

Craig Chambers, Gary T. Leavens

November 1995 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 17 Issue 6

Full text available: pdf(2.90 MB) Additional Information: full citation, references, citings, index terms

Keywords: encapsulation, inheritance, multimethods, static typechecking, subtyping

GROUP, the great majority of which is coded in ANSI Standard FORTRAN. For a discussion of the group theory algorithms planned for the system see Cann ...

4 A language for computational algebra 
Richard D. Jenks, Barry M. Trager
August 1981 **Proceedings of the fourth ACM symposium on Symbolic and algebraic computation**

Full text available: pdf(507.92 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper reports ongoing research at the IBM Research Center on the development of a language with extensible parameterized types and generic operators for computational algebra. The language provides an abstract data type mechanism for defining algorithms which work in as general a setting as possible. The language is based on the notions of domains and categories. Domains represent algebraic structures. Categories designate collections of domains ...

5 Technical contributions: A language for computational algebra 
Richard D. Jenks, Barry M. Trager
November 1981 **ACM SIGPLAN Notices**, Volume 16 Issue 11

Full text available: pdf(543.73 KB) Additional Information: full citation, abstract, references

This paper reports ongoing research at the IBM Research Center on the development of a language with extensible parameterized types and generic operators for computational algebra. The language provides an abstract data type mechanism for defining algorithms which work in as general a setting as possible. The language is based on the notions of *domains* and *categories*. Domains represent algebraic structures. Categories designate collections of domains having common operations with s ...

6 Solving systems of linear one-sided equations in integer monoid and group rings 
Birgit Reinert
July 2000 **Proceedings of the 2000 international symposium on Symbolic and algebraic computation**

Full text available: pdf(183.01 KB) Additional Information: full citation, abstract, references, index terms

One of the applications of Gröbner bases in commutative polynomial rings is to solve linear equations. Here we show how similar results can be obtained for systems of one-sided linear equations in the more general setting of monoid and group rings.

7 An algebraic model for string patterns 
Glenn F. Stewart
January 1975 **Proceedings of the 2nd ACM SIGACT-SIGPLAN symposium on Principles of programming languages**

Full text available: pdf(1.16 MB) Additional Information: full citation, references, citings

8 Proceedings of the SIGNUM conference on the programming environment for development of numerical software 
March 1979 **ACM SIGNUM Newsletter**, Volume 14 Issue 1

Full text available: pdf(5.02 MB) Additional Information: full citation

9 Specifying Concurrent Program Modules 
Leslie Lamport

April 1983 **ACM Transactions on Programming Languages and Systems (TOPLAS)**, Volume 5 Issue 2

Full text available: pdf(2.03 MB) Additional Information: full citation, references, citings, index terms

10 A type system for prototyping languages

Dinesh Katiyar, David Luckham, John Mitchell

February 1994 **Proceedings of the 21st ACM SIGPLAN-SIGACT symposium on Principles of programming languages**

Full text available: pdf(1.36 MB) Additional Information: full citation, abstract, references, citings, index terms

RAPIDE is a programming language framework designed for the development of large, concurrent, real-time systems by prototyping. The framework consists of a type language and default executable, specification and architecture languages, along with associated programming tools. We describe the main features of the type language, its intended use in a prototyping environment, and rationale for selected design decisions.

11 Algebraic invariants of graphs: a study based on computer exploration

Nicolas M. Thiéry

September 2000 **ACM SIGSAM Bulletin**, Volume 34 Issue 3

Full text available: pdf(1.32 MB) Additional Information: full citation, index terms

12 Translations: Solving systems of algebraic equations

Daniel Lazard

September 2001 **ACM SIGSAM Bulletin**, Volume 35 Issue 3

Full text available: pdf(1.63 MB) Additional Information: full citation, abstract, references

Let *f*1,...,*fk* be *k* multivariate polynomials which have a finite number of common zeros in the algebraic closure of the ground field, counting the common zeros at infinity. An algorithm is given and proved which reduces the computations of these zeros to the resolution of a single univariate equation whose degree is the number of common zeros. This algorithm gives the whole algebraic and geometric structure of the set of zeros (multiplicities, conju ...

13 Technical Report Column

Emil Volcheck

June 1997 **ACM SIGSAM Bulletin**, Volume 31 Issue 2

Full text available: pdf(1.11 MB) Additional Information: full citation

14 Unified algebras and modules

P. D. Mosses

January 1989 **Proceedings of the 16th ACM SIGPLAN-SIGACT symposium on Principles of programming languages**

Full text available: pdf(1.52 MB) Additional Information: full citation, abstract, references, index terms

This paper concerns the algebraic specification of abstract data types. It introduces and motivates the recently-developed framework of unified algebras, and provides a practical notation for their modular specification. It also compares unified algebras with the well-known framework of order-sorted algebras, which underlies the OBJ specification language.

15

Genericity versus inheritance
Bertrand Meyer
June 1986 **ACM SIGPLAN Notices , Conference proceedings on Object-oriented programming systems, languages and applications**, Volume 21 Issue 11

Full text available: pdf(1.24 MB) Additional Information: full citation, abstract, references, citings, index terms

Genericity, as in Ada or ML, and inheritance, as in object-oriented languages, are two alternative techniques for ensuring better extendibility, reusability and compatibility of software components. This article is a comparative analysis of these two methods. It studies their similarities and differences and assesses to what extent each may be simulated in a language offering only the other. It shows what features are needed to successfully combine the two approaches in a statically typed l ...

16 Software reuse
Charles W. Krueger
June 1992 **ACM Computing Surveys (CSUR)**, Volume 24 Issue 2

Full text available: pdf(4.96 MB) Additional Information: full citation, abstract, references, citings, index terms

Software reuse is the process of creating software systems from existing software rather than building software systems from scratch. This simple yet powerful vision was introduced in 1968. Software reuse has, however, failed to become a standard software engineering practice. In an attempt to understand why, researchers have renewed their interest in software reuse and in the obstacles to implementing it. This paper surveys the different approaches to software reuse found in the ...

Keywords: abstraction, cognitive distance, software reuse

17 Some algebraic and combinatorial aspects of Multiple-valued circuits
I. G. Rosenberg
May 1976 **Proceedings of the sixth international symposium on Multiple-valued logic**

Full text available: pdf(1.20 MB) Additional Information: full citation, abstract, references, citings, index terms

The purpose of this expository paper is to review some algebraic and combinatorial results arising in the theory of multiple-level switching circuits. Due to space limitations a selection from the surprisingly rich literature had to be made: the trends and topics presented at the past five International Symposia on Multiple-valued logic. The discussion centers on the formulation of basic problems rather than on the presentation of particular results which may be found in a detailed bibliogr ...

18 MPP: a framework for distributed polynomial computations
Olaf Bachmann, Hans Schönemann, Simon Gray
October 1996 **Proceedings of the 1996 international symposium on Symbolic and algebraic computation**

Full text available: pdf(1.23 MB) Additional Information: full citation, references, citings, index terms

19 2W-aray algorithm for extended problem of integer GCD
Hirokazu Murao
March 2000 **ACM SIGSAM Bulletin**, Volume 34 Issue 1

Full text available: pdf(655.01 KB) Additional Information: full citation, index terms

20 A Survey of Some Theoretical Aspects of Multiprocessing
J. L. Baer
January 1973 **ACM Computing Surveys (CSUR)**, Volume 5 Issue 1
Full text available: pdf(4.05 MB) Additional Information: full citation, references, citings, index terms

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next